

**REMARKS**

Favorable reconsideration and allowance of the present application are respectfully requested. Claims 1-3 and 45-51 are pending. Claims 1 and 47 are independent.

**§ 103 REJECTION – SCHNECK, ISHIGURO, CONVENTIONAL ART**

Claims 1-3 and 47-49 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneck et al. (USP 5,933,498) in view of Ishiguro (EP 874300 A2) and in further view of the conventional art described in the specification. Applicants respectfully traverse.

Independent claim 1 recites, in part "generating a key data using at least a unique ID of the digital data playing device" and "encrypting within the source device the digital data file using said key data." The Examiner alleges that Schneck teaches these features.

Contrary to the Examiner's allegation, Schneck does not teach at least the above recited features. More specifically, Schneck discloses a system in which an authoring mechanism 112 (or 148) of the distributor 102 receives data 106. The authoring mechanism 112 also receives access rules 116 that defines the permissions available to the receiver of the data. The authoring mechanism 112 packages the data and the rules by encrypting the data and

the rules with the data key  $K_d$  and the rule key  $K_r$ , respectively. See *Schneck*, Figures 1 and 5; column 9, lines 45-59. *Schneck* clearly discloses that the data 106 is encrypted only with the data encrypting key  $K_d$ . See *Schneck*, Figures 4 and 7; column 12, lines 1-9.

*Schneck* states "the data-encrypting key,  $K_d$ , is "the same for all copies of the data." *Emphasis added*; See *Schneck*, column 12, lines 4-5. In other words, the key used to encrypt the digital data is not based on any unique ID of the digital data playing device. Thus, contrary to the Examiner's allegation, the key data that is used to encrypt the digital data file is not generated based on the unique ID of the digital data playing device at all. Indeed, *Schneck* actually teaches away from this feature.

The rule encrypting key  $K_r$  does not qualify since *Schneck* clearly states that only the data encrypting key  $K_d$  is used to encrypt the data, not the rule encrypting key case of art. Neither Ishiguro nor the conventional art is relied upon to correct for at least this deficiency of *Schneck*. This alone is sufficient to distinguish independent claim 1 from the combination of *Schneck*, Ishiguro and the conventional art.

Claim 1 is also distinguishable for the following reason. The Examiner admits that *Schneck* does not disclose the feature of "transmitting said key data from the digital data playing device to a unit of the source device through a

network" and "a decoding unit configured to decrypt the digital data file read from the data storage medium using said key data." But the Examiner alleges that Ishiguro teaches these features. The Examiner alleges that the DVD player as disclosed in Ishiguro is equivalent to the playing device and that the computer is equivalent to the source device as claimed. The Examiner also alleges that Ishiguro teaches that the DVD player generates and transmits a key to the computer that encrypts data contact in using the transmitted key. The Examiner misapplies the teachings of Ishiguro.

Ishiguro actually teaches the following. As illustrated in Figure 4 and the related description, the DVD player merely includes a service key and a hash function. But neither the service key or the hash function is particular to the DVD player. Therefore, it is impossible for the DVD player to generate an encryption key based on the unique ID of itself.

Indeed, step 1 clearly indicates that the DVD player requests the ID information of the personal computer. Based on the ID information of the personal computer, the DVD player generates a source side common session key sk in step 6. Then, the source side common session key - sk generated in step S6 is encrypted and passed through the computer in step S7.

It is clear that the common source key sk generated by the DVD player is based on the ID of the personal computer, and is **not** based on the unique ID

of the DVD player itself. Clearly, contrary to the Examiner's allegation, Ishiguro cannot teach the feature of transmitting the key data from the digital data playing device to a unit of the source device as recited in claim 1. Indeed, Ishiguro teaches exactly the opposite.

In addition, Ishiguro does not teach that the DVD decrypts any data file from any type of storage medium.

The conventional art is not relied upon to correct for any of the above noted deficiencies of Schneck and Ishiguro. For at least the reasons stated above, it is clear that independent claim 1 is distinguishable over the combination of Schneck, Ishiguro and the conventional art.

Independent claim 47 recites, in part "generating a key data using at least a unique ID of the digital data playing device", "transmitting said key data from the digital data playing device to a unit of the source device" and "encrypting within the source device the digital data file using said key data". It is clear that claim 47 is distinguishable over the combination of Schneck, Ishiguro and the conventional art.

Claims 2-3 and 48-49 depend from independent claims 1 and 47 directly or indirectly. Therefore, for at least due to the dependency thereon, claims 2-3 and 48-49 are also distinguishable over the combination of Schneck, Ishiguro and the conventional art.

Applicants respectfully request that the rejection of claims 1-3 and 47-49 based on Schneck, Ishiguro and the conventional art be withdrawn.

§ 103 REJECTION – SCHNECK, ISHIGURO, MENEZES

Claims 45-46 and 50-51 stand rejected under a combination of Schneck and Ishiguro and in further view of Menezes (Handbook of Applied Cryptography © 1997). Applicants respectfully traverse. Claims 45 and 46 depend from independent claim 1 and claims 50 and 51 depend from independent claim 48. It has been shown above that claims 1 and 48 are distinguishable over the combination of Schneck and Ishiguro. Menezes is not, and indeed cannot be, relied upon to correct for the deficiencies of Schneck and Ishiguro. Therefore, independent claims 1 and 48 are distinguishable over the combination of Schneck, Ishiguro and Menezes.

For at least due to the dependency thereon, claims 45-46 and 50-51 are also distinguishable over the combination of Schneck, Ishiguro and Menezes. Applicants respectfully request that the rejection of claims 45-46 and 50-51 based on Schneck, Ishiguro and Menezes be withdrawn.

Applicants further challenge the Official Notice taken by the Examiner alleging that it is old and well known in the computer networking arts that MP3

devices are used by end users and that generation of encryption keys is accomplished by such devices.

### CONCLUSION


All objections and rejections raised in the Office Action having been addressed, it is respectfully submitted that the present application is in condition for allowance. Should there be any outstanding matters that need to be resolved, the Examiner is respectfully requested to contact Hyung Sohn (Reg. No. 44,346), to conduct an interview in an effort to expedite prosecution in connection with the present application.


If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH &, BIRCH, LLP

By:  #39,538

 Esther H. Chong, #40,953

  
EHC/HNS/ags

P.O. Box 747  
Falls Church, VA 22040-0747  
(703) 205-8000